FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Leonardo Rodrigues Ribeiro

Resumo:

Aplicação de protocolos quânticos e algoritmo de Shor para a segurança da informação

Americana, SP

2023

Introdução

De início o artigo nos mostra que a criptografia clássica corre sérios riscos de segurança por conta da computação quântica, principalmente a assimétrica pois a mesma baseia-se na dificuldade de se solucionar alguns problemas matemáticos e as soluções conhecidas para estes problemas têm complexidade não polinomial que podem ser solucionadas mas com um tamanho de chave aquedada, pode levar centenas de anos mas as computação quântica soluciona isso em pouco tempo, questões de segundos para alguns caso, tal ato seria impossível via computação clássica.

Nos é apresentado também duas classes de algoritmos quânticos com atuações específicas de resolução de problemas, a primeira é baseada na Transformada de Fourier Quântica de Shor e inclui algoritmos notáveis para resolver os problemas de fatoração e de logaritmos discretos com ganho exponencial de velocidade sobre os melhores algoritmos clássicos conhecidos e é usada para decifrar muitos códigos de vários sistemas criptográficos em uso, incluindo o sistema RSA, já a segunda é baseada em Algoritmos de Grover para a realização de busca quântica, que oferece um ganho quadrático de tempo sobre os equivalentes clássicos.

Criptografia

A criptografia RSA baseada na geração de números aleatórios grandes e na operação com números primos entre si (Euler) cria chaves geradas com números muito grandes e primos, fazendo assim com que leve muito tempo para ser decifrada pela computação clássica, mas pela quântica, como citado acima, pode levar segundos, sendo assim o algoritmo de Shor é um fator que apresenta muitos a riscos para a segurança da informação, uma vez que desacelera o tempo exponencial de fatoração com a atual tecnologia para um tempo polinomial, tornando possível decifrar uma mensagem sem possuir a chave privada.

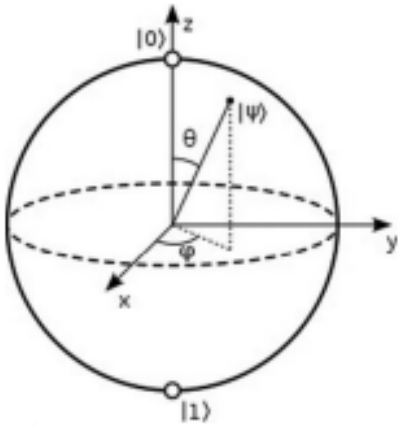
Distribuição de chave quântica

A distribuição de chave quântica é um protocolo provadamente seguro, por meio do qual os bits de uma chave privada podem ser criados por dois parceiros usando um canal público trazendo assim a solução para o problema de distribuição de chaves para a criptografia clássica. A distribuição quântica se torna eficaz pela garantida pelas propriedades da informação quântica e, portanto, condicionada somente às leis da Física, sendo assim, um espião não poderia obter qualquer informação dos qubits transmitidos de A para B sem perturbar o estado compartilhado por eles muito menos realizar o ato de clonagem de bits.

Protocolo BB84

Utiliza os estados de polarização dos fótons para a transmissão de chaves criptográficas, vemos abaixo uma representação pela esfera de Bloch, A e B como os

dois elementos comunicantes e a possibilidade de um espião interceptar a comunicação.



Codificação de forma quântica da sequência $a - b \ \ (4 + 8)n$ bits.

$$|\psi > = \otimes k = 1 \ (4 + \delta)n \ |\psi akbk >$$

ak = k-ésimo bit de a (analogamente para b), e cada qubit está em um dos quatro estados:

$\psi 00 > = |0 >$

$|\ \psi 10 > = |1 >$

$|\ \psi^{01} \ > = \ |+> = \ (|0 \ > \ +|1 \ >)/\sqrt{2}$

$|\ \psi^{11} \ > = \ |-> = \ (|0 \ > \ -|1 \ >)/\sqrt{2}$

Em resumo, o Protocolo BB84 usa qubits e a propriedade quântica da incerteza para criar uma chave secreta compartilhada entre o remetente e o destinatário, permitindo que eles se comuniquem de forma segura mesmo se um intruso tentar interceptar a mensagem, pois se um intruso tentar interceptar a mensagem, a medição dos qubits irá alterar sua polarização, e isso será detectado pelo destinatário, que pode descartar a mensagem. Tem como principais limitações requerimento de canal quântico seguro, dificuldade na implementação prática, tem baixa eficiência e tem vulnerabilidades a ataques laterais como ataques de análise de tráfego, que exploram padrões de transmissão para obter informações sobre a mensagem sendo transmitida.

Para a distribuição de chave quântica(DCQ), o protocolo resolve o problema com um algoritmo *one-time pad*, extremamente seguro. A aplicação desse protocolo é dividida em duas etapas sendo elas a de comunicação quântica e clássica.

Protocolo B92

O Protocolo B92 é um protocolo de criptografia quântica simples que utiliza apenas duas bases de medição para codificar a mensagem e permite a detecção da presença de um intruso, garantindo a segurança da comunicação entre o remetente e o destinatário e a descrição pode facilmente ser generalizada para testes por blocos, como no caso do BB84.

Transformada de Fourier quântica

É uma operação matemática aplicada a qubits em um computador quântico em forma de frequência, sendo essa uma função muito importante na computação atual e o exemplo mais usual é o reconhecimento de fala no qual é usado esse algoritmo em sons digitalizados.

Algoritmo de fatoração de Shor

Atualmente, é considerado um dos melhores algoritmos para fatoração, pois na versão quântica é capaz de fatorar números de altas ordens em segundos, então muitos dos sistemas criptográficos atuais seriam quebrados com por exemplo o RSA, o que tem implicações significativas para a segurança de informações confidenciais. Exemplo prático:

1. $-\ escolha\ um\ inteiro\ 1\ <\ x\ <n\ aleatoriamente$
2. $-\ se\ mdc(x,n)\ >\ 1$
3. $-\ então\ devolva\ mdc(x,n)$
4. $-\ seja\ r\ o\ período\ da\ função\ f(a)\ = xa\ mod\ n$
5. $-\ se\ r\ for\ ímpar\ ou\ xr/2\ \equiv\ -1(mod\ n)$
6. $-\ então\ o\ procedimento\ falhou$
7. $-\ devolva\ mdc(xr/2\ +\ 1,n)$

Implementação em Javascript

Javascript se diferencia por permitir o desenvolvimento dos códigos dentro do código HTML. Para o desenvolvedor, seu uso é muito simples: é só adicionar o código "$<scrpit>$" e iniciar a programação na linguagem referenciada. Para implementar o algoritmo quântico de Shor, utilizou-se a biblioteca Jsqubits, da linguagem de programação Javascript, sendo esse algoritmo desenvolvido em node.js e Javascript es6.

Abaixo vemos exemplos dessa implementação:

```
//Nesta condição, as chances de obter uma resposta obviamente erradas são reduzidas a partir
//da verificação se o fator comum aleatório obtido a partir da função que gera um numero primo
//está no intervalo > 1 e < que o número que queremos descobrir seus fatores.
if (candidateDivisor > 1 && candidateDivisor <= outputRange) {
  if (f(candidateDivisor) === f0) {
    console.log('This is a multiple of the rank.');
    bestSoFar = candidateDivisor;
  } else {
    var lcm = jsqubitsmath.lcm(candidateDivisor, bestSoFar);
    if (lcm <= outputRange) {
      console.log('This is a good candidate.');
      bestSoFar = lcm;
    }
```

```
//Essa condição retorna imediatamente o fator comum '2' caso o número colocado seja par
if (n % 2 === 0) {
  // Is even.  No need for any quantum computing!
  return 2;
}
```

```
//Nessa condição, é verificado se a função powerfactor retorna um número > 1, caso sim
// dentro da função do powerfactor ele verifica se o n (número fatorado) possui
// é um powerfactor. O powerfactor nada mais é que um primo multiplicado por ele mesmo X vezes resultado em n.
var powerFactor = jsqubitsmath.powerFactor(n);
if (powerFactor > 1) {
  // Is a power factor.  No need for anything quantum!
  return powerFactor;
}
```

```
//essa parte do código captura o horário em que dá o 'start' armazenando o horario atual em uma
//variavel para achar os fatores comuns e, ao final, quando o resultado é exibido,
//chama-se uma função que retorna o horario atual e depois substitui pelo valor da variavel
//que armazena o horario em que foi iniciado a busca/1000, retornando em segundos
//o tempo levado pela a operação.
var startTime = new Date();
factor(n, function(result) {
    log("One of the factors of " + n + " is " + result);
    log("Time taken in seconds: " + ((new Date().getTime()) - startTime.getTime()) / 1000);
});
```

Conclusão

Conclui-se que a distribuição de chaves na computação clássica está totalmente fragilizada com a chegada da computação quântica tendo como exemplo o algoritmo de Shor que tem implicações importantes na criptografia, pois ele pode fatorar rapidamente números grandes, o que pode quebrar muitos dos sistemas criptográficos atuais como a RSA por exemplo. No entanto, ele só pode ser executado em um computador quântico, o que significa que ainda há uma grande limitação para sua aplicação prática, deixando assim a fragilidade da computação clássica exposta e sem segurança alguma para tais ataques.

Temos os BB84 e B92 que usa a propriedade quântica de entrelaçamento para garantir a segurança da transmissão de informação, por apresentação foi mostrado como garantir a segurança do uso de um canal de comunicação, uma vez que através

desses protocolos, tem-se a certeza se a informação sofreu ou não espionagem, e de que não foi clonada. A transformada de Fourier quântica é outro fator importante citado pois por ele conseguimos ter o reconhecimento de fala no qual é usado esse algoritmo em sons digitalizados, mas assim como a de Shor, tem suas limitações pois requerem canal quântico seguro, há dificuldade na implementação prática, tem baixa eficiência e tem vulnerabilidades a ataques laterais como ataques de análise de tráfego, que exploram padrões de transmissão para obter informações sobre a mensagem sendo transmitida.

É nos mostrado também a implementação do Algoritmo de fatoração de Shor, através da linguagem Javascript apenas como ilustração do Algoritmo, mostra o lado “prático” e “tangível” da aplicação dos conceitos quânticos atualmente, mesmo que até o momento, a implementação prática de qubits é possível apenas em hardware quântico, o que significa que a implementação do algoritmo de fatoração de Shor em Javascript seria apenas uma simulação.